UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/806,668	03/23/2004	Russell Wayne Dellmo	GCSD-1573 (51395)	1171

74701 7590 01/04/2011

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO, FL 32801

EXAMINER	
PAN, JOSEPH T	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
01/04/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	Application No.	Applicant(s)	
	10/806,668	DELLMO ET AL.	
	Examiner	Art Unit	
	JOSEPH PAN	2492	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,11-18 and 21-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,11-18 and 21-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's response filed on October 25, 2010 has been fully considered. Claim 38 has been amended. Claims 1-8, 11-18, and 21-38 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-8, 11-18, 21-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dhir et al. (U.S. Patent No. 7,142,557 B2), hereinafter "Dhir", in view of Cheng (U.S. Pub. No. 2003/0221034 A1), and further in view of Vos (U.S. Patent No. 4,849,927).

Referring to claim 1:

i. Dhir teaches:

A cryptographic device comprising:

a cryptographic module and a communications module (see figure 8, elements 321 'encryption engine', 301 'wlan [i.e., wireless local area network] transceiver' of Dhir);

said cryptographic module comprising

a user Local Area Network (LAN) network interface (see figure 8, elements 325 'host bus interface', 326 'host device interface'; and figure 9, element 335 'LAN', of Dhir),

a cryptographic processor coupled to said user Local Area Network (LAN) interface (see figure 8, element 321 'encryption engine' of Dhir),

said communications module comprising

a network wireless LAN interface (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver' of Dhir), coupled to said cryptographic processor and switchable between wireless LAN modes (see column 3, lines 1-17 of Dhir).

Dhir further discloses that the cryptographic module and the communication module are separable (see column 7, lines 48-56 'In this embodiment, a **separate** transceiver 301 integrated circuit [i.e., the communication module], namely not embedded in FPGA 300, is coupled to FPGA 300 [i.e., the cryptographic module], as is program memory 312.', of Dhir). However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a tampering circuit for disabling said cryptographic processor based upon tampering with the housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing.

ii. Cheng teaches an add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable [i.e., removably coupled] from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng, emphasis added).

On the other hand, Vos teaches a method of controlling the operation of security module wherein Vos discloses a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing so that said cryptographic processor is disabled based upon a break in said at least one conductive trace (see figure 7; and col. 3, lines 58-64 'Each of the six plates [i.e., the housing] has provided thereon a pair of conductive path segments [i.e., the conductive trace printed on the housing] (not shown), the conductive path segments on the respective plates P1-P6 being joined together to form two wire meshes. The wire

meshes are connected to tamper detection circuitry [i.e., the tamper circuit comprising at least one conductive trace printed on the housing] for protecting the security module 10 against unauthorized tampering,'; col. 5, line 57, to col. 6, line 10 'Referring to FIG. 7, the algorithm is effected in m time periods T.sub.1,T.sub.2, . . . ,T.sub.m. During time period T.sub.1, the 64-bit block F.sub.1 is applied as an input I.sub.1 (block 100) to the DEA (Data Encryption Algorithm) (block 102), using KA as the DES key [i.e., KA (authentication key) is used as an encryption key for the cryptographic processor]...'; and col. 7, lines 30-42 'It will be noted that any attempt to tamper with or break into the security module will result in the generation of the RESET signal [i.e., generating a signal upon detecting tampering with the housing] on the lead 52 (FIG. 3). Such RESET signal is effective to reset the resettable shift register 54 and hence erase the key storage key KSK. With KSK erased, the authentication key KA, stored in the secure memory 36 as KAENCR becomes unavailable [i.e., KA (authentication key, used as the encryption key) becomes unavailable because the key storage key KSK is erased, thus the cryptographic processor in figure 7 becomes disabled] since it cannot be decrypted, and hence the security module 10 can no longer be loaded with new firmware...', of Vos, emphasis added).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Vos into the system of Dhir to use the tampering circuit for disabling said cryptographic processor based upon tampering, because Dhir teaches "Another aspect of the present invention is the above method further comprising storing a plurality of encryption algorithms configured to program the configuration logic blocks, and selectively programming a second portion of a configuration logic blocks with an encryption algorithm selected from the plurality of encryption algorithms [i.e., a cryptographic processor]." (see column 3, lines 11-17, of Dhir, emphasis added). Vos

teaches "Security modules have found application in data processing systems and networks where a high degree of security is important. Such applications include electronic payment systems, electronic funds transfer (EFT) systems, data encryption and decryption, PIN (personal identification number) verification, access control and home banking." (see column 1, lines 18-24, of Vos, emphasis added). Therefore, Vos's teaching would enhance Dhir's system, because Vos's "Security modules have found application in data processing systems and networks where a high degree of security is important".

Referring to claims 2, 12, 22, 26, 30:

Dhir, Cheng, and Vos teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose that the network wireless LAN interface circuit is switchable to one of an access point (AP) mode, an infrastructure mode, and an ad-hoc mode (see figure 9; and column 3, lines 1-17 of Dhir).

Referring to claims 3, 13, 23, 27, 31:

Dhir, Cheng, and Vos teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the connector (see figure 4, element 55A, 55B, 57A, 57B of Cheng).

Referring to claims 4, 14, 24, 28, 32:

Dhir, Cheng, and Vos teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the Ethernet (see column 2, lines 18 of Dhir).

Referring to claims 5, 15, 33:

Dhir, Cheng, and Vos teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the power (see page 3, paragraph [0030], lines 10-13 of Cheng).

Referring to claims 6, 16, 34:

Dhir, Cheng, and Vos teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the encryption algorithm (see column 9, lines 19-20 of Dhir).

Referring to claims 7, 17, 35:

Dhir, Cheng, and Vos teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the processor and the encryption circuit (see figure 8, elements 324 'baseband processor', 321 'encryption engine' of Dhir).

Referring to claims 8, 18, 36:

Dhir, Cheng, and Vos teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the data buffer (see page 1, paragraph [0009], line 6-end, of Cheng).

Referring to claim 11:

i. Dhir teaches:

A cryptographic device comprising:

a cryptographic module and a communications module (see figure 8, elements 321 'encryption engine', 301 'wlan transceiver' of Dhir);

said cryptographic module comprising

a user local area network interface (LAN) (see figure 8, elements 325 'host bus interface', 326 'host device interface'; and figure 9, element 335 'LAN', of Dhir),

a cryptographic processor coupled to said user LAN interface (see figure 8, element 321 'encryption engine' of Dhir), and

said communications module comprising

a network wireless LAN interface (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver' of Dhir), and

said communications module comprising a predetermined one from among a plurality of interchangeable communications modules, and said network wireless LAN interfaces of said plurality of interchangeable communications modules each operating using a different wireless LAN mode (see column 3, lines 1-17 of Dhir).

Dhir further discloses that the cryptographic module and the communication module are separable (see column 7, lines 48-56 'In this embodiment, a **separate** transceiver 301 integrated circuit [i.e., the communication module], namely not embedded in FPGA 300, is coupled to FPGA 300 [i.e., the cryptographic module], as is

program memory 312.', of Dhir). However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a tampering circuit for disabling said cryptographic processor based upon tampering with the housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing.

ii. Cheng teaches an add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable [i.e., removably coupled] from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng, emphasis added).

On the other hand, Vos teaches a method of controlling the operation of security module wherein Vos discloses a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing so that said cryptographic processor is disabled based upon a break in said at least one conductive trace (see figure 7; and col. 3, lines 58-64 'Each of the six plates [i.e., the housing] has provided thereon a pair of conductive path segments [i.e., the conductive trace printed on the housing] (not shown), the conductive path segments on the respective plates P1-P6 being joined together to form two wire meshes. The wire meshes are connected to tamper detection circuitry [i.e., the tamper circuit comprising at least one conductive trace printed on the housing] for protecting the security module 10 against unauthorized tampering,'; col. 5, line 57, to col. 6, line 10 'Referring to FIG. 7, the algorithm is effected in m time periods T.sub.1,T.sub.2, . . . ,T.sub.m. During time period T.sub.1, the 64-bit block F.sub.1 is applied as an input I.sub.1 (block 100) to the DEA (Data Encryption Algorithm) (block 102), using KA as the DES key [i.e., KA (authentication key) is used as an encryption key for the cryptographic processor]...'; and col. 7, lines 30-42 'It will be noted that any attempt to tamper with or break into the security module will result in the generation of the RESET signal [i.e., generating a signal upon detecting tampering with the housing] on the lead 52 (FIG. 3). Such RESET signal is effective to reset the resettable shift register 54 and hence erase the

key storage key KSK. With KSK erased, the authentication key KA, stored in the secure memory 36 as KAENCR becomes unavailable [i.e., KA (authentication key, used as the encryption key) becomes unavailable because the key storage key KSK is erased, thus the cryptographic processor in figure 7 becomes disabled] since it cannot be decrypted, and hence the security module 10 can no longer be loaded with new firmware...', of Vos, emphasis added).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Vos into the system of Dhir to use the tampering circuit for disabling said cryptographic processor based upon tampering, because Dhir teaches "Another aspect of the present invention is the above method further comprising storing a plurality of encryption algorithms configured to program the configuration logic blocks, and selectively programming a second portion of a configuration logic blocks with an encryption algorithm selected from the plurality of encryption algorithms [i.e., a cryptographic processor]." (see column 3, lines 11-17, of Dhir, emphasis added). Vos teaches "Security modules have found application in data processing systems and networks where a high degree of security is important. Such applications include electronic payment systems, electronic funds transfer (EFT) systems, data encryption and decryption, PIN (personal identification number) verification, access control and home banking." (see column 1, lines 18-24, of Vos, emphasis added). Therefore, Vos's teaching would enhance Dhir's system, because Vos's "Security modules have found application in data processing systems and networks where a high degree of security is important".

Referring to claim 21:

i. Dhir teaches:

A communications method comprising:

coupling a cryptographic module to a Local Area Network (LAN) device, a cryptographic processor coupled to the user LAN interface (see figure 8, element 321 'encryption engine'; and figure 9, element 335 'LAN', of Dhir);

providing a communications module, a network wireless LAN interface (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver', of Dir);

using the network wireless LAN interface to communicate with a wireless LAN (see column 6, line 66-column 7, line 3 of Dhir).

Dhir further discloses that the cryptographic module and the communication module are separable (see column 7, lines 48-56 'In this embodiment, a **separate** transceiver 301 integrated circuit [i.e., the communication module], namely not embedded in FPGA 300, is coupled to FPGA 300 [i.e., the cryptographic module], as is program memory 312.', of Dhir). However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a tampering circuit for disabling said cryptographic processor based upon tampering with the housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing.

ii. Cheng teaches an add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable [i.e., removably coupled] from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng, emphasis added).

On the other hand, Vos teaches a method of controlling the operation of security module wherein Vos discloses a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing so that said cryptographic processor is disabled based upon a break in said at least one conductive trace (see figure 7; and col. 3, lines 58-64 'Each of the six plates [i.e., the housing] has provided thereon a pair of conductive path segments [i.e., the conductive trace printed on the housing] (not shown), the conductive path segments on

the respective plates P1-P6 being joined together to form two wire meshes. The wire meshes are connected to tamper detection circuitry [i.e., the tamper circuit comprising at least one conductive trace printed on the housing] for protecting the security module 10 against unauthorized tampering,'; col. 5, line 57, to col. 6, line 10 'Referring to FIG. 7, the algorithm is effected in m time periods T.sub.1,T.sub.2, . . . ,T.sub.m. During time period T.sub.1, the 64-bit block F.sub.1 is applied as an input I.sub.1 (block 100) to the DEA (Data Encryption Algorithm) (block 102), using KA as the DES key [i.e., KA (authentication key) is used as an encryption key for the cryptographic processor]...'; and col. 7, lines 30-42 'It will be noted that any attempt to tamper with or break into the security module will result in the generation of the RESET signal [i.e., generating a signal upon detecting tampering with the housing] on the lead 52 (FIG. 3). Such RESET signal is effective to reset the resettable shift register 54 and hence erase the key storage key KSK. With KSK erased, the authentication key KA, stored in the secure memory 36 as KAENCR becomes unavailable [i.e., KA (authentication key, used as the encryption key) becomes unavailable because the key storage key KSK is erased, thus the cryptographic processor in figure 7 becomes disabled] since it cannot be decrypted, and hence the security module 10 can no longer be loaded with new firmware...', of Vos, emphasis added).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Vos into the system of Dhir to use the tampering circuit for disabling said cryptographic processor based upon tampering, because Dhir teaches "Another aspect of the present invention is the above method further comprising storing a plurality of encryption algorithms configured to program the configuration logic blocks, and selectively programming a second portion of a configuration logic blocks with an encryption algorithm selected from the plurality of encryption algorithms [i.e., a

cryptographic processor]." (see column 3, lines 11-17, of Dhir, emphasis added). Vos teaches "Security modules have found application in data processing systems and networks where a high degree of security is important. Such applications include electronic payment systems, electronic funds transfer (EFT) systems, data encryption and decryption, PIN (personal identification number) verification, access control and home banking." (see column 1, lines 18-24, of Vos, emphasis added). Therefore, Vos's teaching would enhance Dhir's system, because Vos's "Security modules have found application in data processing systems and networks where a high degree of security is important".

Referring to claim 25:

i. Dhir teaches:

A communications method comprising:

coupling a cryptographic module to a Local Area Network (LAN) device, a cryptographic processor coupled to the user LAN interface; coupling the user LAN interface to a LAN device (see figure 8, element 321 'encryption engine'; and figure 9, element 335 'LAN', of Dhir);

coupling one of a plurality of communication modules to the cryptographic module, and the network wireless LAN interfaces of the plurality of interchangeable communications modules each operating in a different wireless LAN mode (see figure 8, element 321 'encryption engine', element 301 'wlan [i.e., wireless local area network]; column 3, lines 1-17; and column 6, line 66-column 7, line 3 of Dhir); and

using the communications module to communicate with a wireless LAN (see figure 8, element 301 'wlan [i.e., wireless local area network]; and column 6, line 66-column 7, line 3 of Dhir).

Dhir further discloses that the cryptographic module and the communication module are separable (see column 7, lines 48-56 'In this embodiment, a **separate** transceiver 301 integrated circuit [i.e., the communication module], namely not embedded in FPGA 300, is coupled to FPGA 300 [i.e., the cryptographic module], as is program memory 312.', of Dhir). However, Dhir does not specifically mention that the

cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a tampering circuit for disabling said cryptographic processor based upon tampering with the housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing.

ii. Cheng teaches an add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable [i.e., removably coupled] from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng, emphasis added).

On the other hand, Vos teaches a method of controlling the operation of security module wherein Vos discloses a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing so that said cryptographic processor is disabled based upon a break in said at least one conductive trace (see figure 7; and col. 3, lines 58-64 'Each of the six plates [i.e., the housing] has provided thereon a pair of conductive path segments [i.e., the conductive trace printed on the housing] (not shown), the conductive path segments on the respective plates P1-P6 being joined together to form two wire meshes. The wire meshes are connected to tamper detection circuitry [i.e., the tamper circuit comprising at least one conductive trace printed on the housing] for protecting the security module 10 against unauthorized tampering,'; col. 5, line 57, to col. 6, line 10 'Referring to FIG. 7, the algorithm is effected in m time periods T.sub.1,T.sub.2, . . . ,T.sub.m. During time period T.sub.1, the 64-bit block F.sub.1 is applied as an input I.sub.1 (block 100) to the DEA (Data Encryption Algorithm) (block 102), using KA as the DES key [i.e., KA (authentication key) is used as an encryption key for the cryptographic processor]...'; and col. 7, lines 30-42 'It will be noted that any attempt to tamper with or break into the security module will result in the generation of the RESET signal [i.e., generating a signal upon detecting tampering with the housing] on the lead 52 (FIG. 3). Such RESET signal is effective to reset the resettable shift register 54 and hence erase the key storage key KSK. With KSK erased, the authentication key KA, stored in the secure

memory 36 as KAENCR becomes unavailable [i.e., KA (authentication key, used as the encryption key) becomes unavailable because the key storage key KSK is erased, thus the cryptographic processor in figure 7 becomes disabled] since it cannot be decrypted, and hence the security module 10 can no longer be loaded with new firmware...', of Vos, emphasis added).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Vos into the system of Dhir to use the tampering circuit for disabling said cryptographic processor based upon tampering, because Dhir teaches "Another aspect of the present invention is the above method further comprising storing a plurality of encryption algorithms configured to program the configuration logic blocks, and selectively programming a second portion of a configuration logic blocks with an encryption algorithm selected from the plurality of encryption algorithms [i.e., a cryptographic processor]." (see column 3, lines 11-17, of Dhir, emphasis added). Vos teaches "Security modules have found application in data processing systems and networks where a high degree of security is important. Such applications include electronic payment systems, electronic funds transfer (EFT) systems, data encryption and decryption, PIN (personal identification number) verification, access control and home banking." (see column 1, lines 18-24, of Vos, emphasis added). Therefore, Vos's teaching would enhance Dhir's system, because Vos's "Security modules have found application in data processing systems and networks where a high degree of security is important".

Referring to claim 29:

i. Dhir teaches:

A communications system comprising:

a plurality of Local Area Network (LAN) devices coupled together to define a network, and a cryptographic device coupled to at least one of said LAN devices (see figure 9, element 335 'LAN'; and figure 8, element 321 'encryption engine', of Dhir);

said cryptographic device comprising a cryptographic module coupled to said at least one LAN device, and a communications module (see figure 8, element 321 'encryption engine', element 301 'wlan [i.e., wireless local area network] transceiver' of Dhir);

said cryptographic module comprising a cryptographic processor coupled to said user LAN interface (see figure 8, element 321 'encryption engine', element 325 'host bus interface', element 326 'host device interface' of Dhir);

said communications module comprising a network wireless LAN communications interface, coupled to the cryptographic processor and switchable between wireless LAN modes (see figure 8, element 301 'transceiver'; and column 3, lines 1-17, of Dhir).

Dhir further discloses that the cryptographic module and the communication module are separable (see column 7, lines 48-56 'In this embodiment, a **separate** transceiver 301 integrated circuit [i.e., the communication module], namely not embedded in FPGA 300, is coupled to FPGA 300 [i.e., the cryptographic module], as is program memory 312.', of Dhir). However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a tampering circuit for disabling said cryptographic processor based upon tampering with the housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing.

ii. Cheng teaches an add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable [i.e., removably coupled] from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng, emphasis added).

On the other hand, Vos teaches a method of controlling the operation of security module wherein Vos discloses a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing, said tamper circuit comprising at least one conductive trace printed on at least the inside of said first housing so that said cryptographic processor is disabled based upon a break in said at least one conductive trace (see figure 7; and col. 3, lines 58-64 'Each of the six plates [i.e., the housing] has provided thereon a pair of conductive path segments [i.e., the conductive trace printed on the housing] (not shown), the conductive path segments on the respective plates P1-P6 being joined together to form two wire meshes. The wire meshes are connected to tamper detection circuitry [i.e., the tamper circuit comprising at least one conductive trace printed on the housing] for protecting the security module 10 against unauthorized tampering,'; col. 5, line 57, to col. 6, line 10 'Referring to FIG. 7, the algorithm is effected in m time periods T.sub.1,T.sub.2, . . . ,T.sub.m. During time period T.sub.1, the 64-bit block F.sub.1 is applied as an input I.sub.1 (block 100) to the DEA (Data Encryption Algorithm) (block 102), using KA as the DES key [i.e., KA (authentication key) is used as an encryption key for the cryptographic processor]...'; and col. 7, lines 30-42 'It will be noted that any attempt to tamper with or break into the security module will result in the generation of the RESET signal [i.e., generating a signal upon detecting tampering with the housing] on the lead 52 (FIG. 3). Such RESET signal is effective to reset the resettable shift register 54 and hence erase the key storage key KSK. With KSK erased, the authentication key KA, stored in the secure memory 36 as KAENCR becomes unavailable [i.e., KA (authentication key, used as the encryption key) becomes unavailable because the key storage key KSK is erased, thus the cryptographic processor in figure 7 becomes disabled] since it cannot be decrypted, and hence the security module 10 can no longer be loaded with new firmware...', of Vos, emphasis added).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection

module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Vos into the system of Dhir to use the tampering circuit for disabling said cryptographic processor based upon tampering, because Dhir teaches "Another aspect of the present invention is the above method further comprising storing a plurality of encryption algorithms configured to program the configuration logic blocks, and selectively programming a second portion of a configuration logic blocks with an encryption algorithm selected from the plurality of encryption algorithms [i.e., a cryptographic processor]." (see column 3, lines 11-17, of Dhir, emphasis added). Vos teaches "Security modules have found application in data processing systems and networks where a high degree of security is important. Such applications include electronic payment systems, electronic funds transfer (EFT) systems, data encryption and decryption, PIN (personal identification number) verification, access control and home banking." (see column 1, lines 18-24, of Vos, emphasis added). Therefore, Vos's teaching would enhance Dhir's system, because Vos's "Security modules have found application in data processing systems and networks where a high degree of security is important".

4. Claims 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dhir et al. (U.S. Patent No. 7,142,557 B2), in view of Cheng (U.S. Pub. No. 2003/0221034 A1), further in view of Vos (U.S. Patent No. 4,849,927), and further in view of Allmond et al. (U.S. Patent No. 5,754,552), hereinafter "Allmond".

Referring to claims 37-38:

i. Dhir, Cheng, and Vos teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the connector (see page 1, paragraph [0017], lines 13-16, of Cheng). However, They do not specifically mention a plurality of connectors.

ii. On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 to column 11, line 24 of Allmond).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir, Cheng, and Vos to use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a multi-platform wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of a plurality of communication protocols (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance the system of Dhir, Cheng, and Vos.

Response to Arguments

5. Applicant's arguments filed on October 25, 2010, with respect to that the references do not disclose the tamper circuit disabling the cryptographic processor based on the tampering with the housing, have been fully considered and they are persuasive. Therefore, the rejection has been withdrawn. However, upon a further consideration, a new ground(s) of rejection is made in view Vos.

(a) Applicant states:

"Additionally, Applicants submit that the Examiner's combination of references is improper. More particularly, a person having ordinary skill in the art would not turn to Cheng to combine with Dhir et al. and Hamlin to arrive at the claimed invention. As an initial matter, Dhir et al. is directed to a programmable logic device for a WLAN. The communications module and the cryptographic module are purposely on a single circuit

board (330), as illustrated in Fig. 8 of Dhir et ai. Combining Dhir et al. with Cheng so that the communications module and the cryptographic module would be removably coupled would require splitting the communications and cryptographic modules from the single circuit board." (see page 19, 2nd paragraph)

Examiner states:

An a initial matter, Hamlin is not used as a reference in the previous Office action.

Dhir discloses "Referring to FIG. 7, there is shown an exemplary embodiment of FPGA 300 program in accordance with one or more aspects of the present invention. In this embodiment, a **separate** transceiver 301 integrated circuit [i.e., the communication module] , namely not embedded in FPGA 300, **is coupled** to FPGA 300 [i.e., the cryptographic module], as is program memory 312. In this embodiment, a direct interface between **separate** transceiver 301 and FPGA 300 may be employed for direct interaction between transceiver 301 and FPGA 300." (see column 7, lines 48-56, of Dhir, emphasis added). Therefore, Dhir discloses that the transceiver 301 [i.e., the communication module] is removably coupled to the FPGA 300 [i.e., the cryptographic module]. However, Dhir does not explicitly disclose that the transceiver 301 [i.e., the communication module] is detachable from the FPGA 300 [i.e., the cryptographic module].

On the other hand, Chen discloses "[0029] Please refer to FIG. 4. FIG. 4 is a functional block diagram of the add-on card 50 [i.e., the circuit board] connected with the portable computer 12. The first portion 51A [i.e., the first housing] of the add-on card 50 includes an access control circuit MAC2, a volatile memory M3, and a non-volatile memory M4. The first portion 51A also has a base frequency circuit 66A, an intermediate frequency circuit 66B, and a radio frequency circuit 66C all of a wireless transmission module 64.The second portion 51B [i.e., the second housing, consisting of the communication module] includes an antenna circuit ANT2 and a connecting circuit PHY2, both of a network connection module 68. All these components in both sections of the add-on card 50 have the same function as those with the same names in the add-on card 10 and operate in the same manner together. The key difference between the

add-on card 50 and the add-on card 10 is that the components of the add-on card 50 [i.e., the circuit board] are **separated** into the **detachable** first portion 51A [i.e., the first housing] and second portion 51B [i.e., the second housing, consisting of the communication module]. In the add-on card 50, the network connection module 68 is installed in the second portion 51B, and the remaining components are installed in the first port 51A. The transmission ports 53A and 53B of the first portion 51A and second portion 51B respectively comprise first sub-transmission ports 55A, 55B and second sub-transmission ports 57A, 57B. The wireless transmission module 64 in the first portion 51A is connected to the antenna circuit ANT2 in the second portion 51B via the first sub-transmission ports 55A and 55B. The access control circuit MAC2 in the first portion 51A is connected to the connecting circuit PHY2 in the second portion 51B via the second sub-transmission ports 57A and 57B." (see figure 4; and page 3, paragraph [0029], of Chen, emphasis added). Therefore, Chen discloses that the add-on card [i.e., the circuit board] is **separated** into the **detachable** first portion 51A [i.e., the first housing] and second portion 51B [i.e., the second housing, consisting of the communication module].

Thus, the combination of Dhir and Chen disclose a cryptographic module and a communication module removably coupled, such as disclosed in the claimed invention.

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

(a) Beiley et al. (U.S. Patent No. 7,024,565 B1) disclose a method and apparatus to detect circuit tampering.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached at 571-272-6776. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Zachary A Davis/
Primary Examiner, Art Unit 2492

/Joseph Pan/
Examiner, Art Unit 2492
December 20, 2010